1994

Improving the strict avalanche characteristics of cryptographic functions

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Xian-Mo Zhang
University of Wollongong, xianmo@uow.edu.au

Yuliang Zheng
University of Wollongong, yuliang@uow.edu.au

Improving the strict avalanche characteristics of cryptographic functions

Abstract

This paper presents a simple yet effective method for transforming Boolean functions that do not satisfy the strict avalanche criterion (SAC) into ones that satisfy the criterion. Such a method has a wide range of applications in designing cryptographically strong functions, including substitution boxes (S-boxes) employed by common key block encryption algorithm.

Publication Details

Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng, Improving the strict avalanche characteristics of cryptographic functions, Information Processing Letters, 50, (1994), 37-41.

Improving the Strict Avalanche Characteristics of Cryptographic Functions *

Jennifer Seberry

Xian-Mo Zhang

Yuliang Zheng

The Centre for Computer Security Research

Department of Computer Science

The University of Wollongong

Wollongong, NSW 2522, AUSTRALIA

E-mail: {jennie,xianmo,yuliang}@cs.uow.edu.au

Abstract

This paper presents a simple yet effective method for transforming Boolean functions that do not satisfy the strict avalanche criterion (SAC) into ones that satisfy the criterion. Such a method has a wide range of applications in designing cryptographically strong functions, including substitution boxes (S-boxes) employed by common key block encryption algorithms.

*The first author was supported in part by the Australian Research Council under the reference numbers A49130102, A9030136, A49131885 and A49232172, the second author by A49130102, and the third author by A49232172.

Key Words

cryptography, security in digital systems, strict avalanche criterion (SAC), substitution boxes (S-boxes).

1 The Strict Avalanche Criterion

A (Boolean) function on V_n, where V_n denotes the the vector space of n-tuples of elements from $GF(2)$, is said to satisfy the strict avalanche criterion (SAC) if complementing a single bit in its input results in the output of the function being complemented half the time over all the input vectors. The SAC is one of the most important requirements for cryptographic functions. The formal definition for the SAC seems to appear first in the open literature in 1985 [11, 12]:

Definition 1 *Let f be a function on V_n. f is said to satisfy the SAC if $f(x) \oplus f(x \oplus \alpha)$ assumes the values zero and one an equal number of times, or simply, $f(x) \oplus f(x \oplus \alpha)$ is balanced, for every $\alpha \in V_n$ with $W(\alpha) = 1$, where $x = (x_1, \ldots, x_n)$ and $W(\alpha)$ denotes the number of ones in (or the Hamming weight of) the vector α.*

The SAC has been further generalized in two different directions: high order SAC and propagation criterion. The first direction is represented by [4], while the second by [1, 8, 7]. We shall not pursue further these developments in this paper. Instead we will focus our attention on how to transform functions which do not satisfy the SAC into ones that satisfy the criterion.

2 Single Functions

First we introduce the following basic theorem.

Theorem 1 *Let f be a function on V_n, and A be a nondegenerate matrix of order n whose entries are from $GF(2)$. Suppose that $f(x) \oplus f(x \oplus \gamma_i)$ is balanced for each row γ_i of A, where $i = 1, \ldots, n$ and $x = (x_1, \ldots, x_n)$. Then $\psi(x) = f(xA)$ satisfies the SAC.*

Proof. Let δ_i be a vector in V_n whose entries, *except the ith*, are all zero. Note that $W(\delta_i) = 1$ and $\delta_i A = \gamma_i$, $i = 1, \ldots n$. Then we have $\psi(x) \oplus \psi(x \oplus \delta_i) = f(xA) \oplus f((x \oplus \delta_i)A) = f(u) \oplus f(u \oplus \gamma_i)$, where $u = xA$. Since A is nondegenerate, u runs through V_n while x does. By assumption, $f(u) \oplus f(u \oplus \gamma_i)$ runs through the values zero and one an equal number of times while u runs through V_n. Consequently $\psi(x) \oplus \psi(x \oplus \delta_i)$ runs through the values zero and one an equal number of times while x runs through V_n. That is, $\psi(x)$ satisfies the SAC. □

Note that the algebraic degree, the nonlinearity and the balancedness of a function is unchanged under a linear transformation of coordinates [13]. In the case of S-boxes (tuples of functions), the profile of its XOR distribution table, which measures the strength against the differential cryptanalysis [2], also remains invariant under such a transformation [10]. Thus Theorem 1 provides us a powerful tool to improve the strict avalanche characteristics of cryptographic functions. In the following we consider two applications of the theorem.

Application 1 Our first application shows that a SAC-fulfilling function on a higher dimensional space can be easily obtained from a SAC-fulfilling function on a lower dimensional space.

Let $g(y_1, \ldots, y_s)$ be a function on V_s that satisfies the SAC. Adding t pseudo-coordinates $x_1, \ldots, x_t$ into g, we obtain a function f on V_{s+t}, namely,

$$f(y_1, \ldots, y_s, x_1, \ldots, x_t) = g(y_1, \ldots, y_s)$$

The t newly added coordinates have no influence on the output of f. Hence f does not satisfy the SAC.

Let A be a nondegenerate matrix of order $s + t$. Assume that each row γ_i of A can be written as $\gamma_i = (\beta_i, \alpha_i)$, where $W(\beta) = 1$, $\beta_i \in V_s$ and $\alpha_i \in V_t$. Let $x = (x_1, \ldots, x_t)$, $y = (y_1, \ldots, y_s)$ and $z = (y, x)$. Then we have $f(z) \oplus f(z \oplus \gamma_i) = g(y) \oplus g(y \oplus \beta_i)$. This shows that $f(z) \oplus f(z \oplus \gamma_i)$ is balanced for γ_i, $i = 1, \ldots, s + t$. By Theorem 1, $\psi(z) = f(zA)$ satisfies the SAC.

An example of the matrices that satisfy the requirements is as follows:

$$A = \begin{bmatrix} I_s & 0_{s\times t} \\ Q_{t\times s} & I_t \end{bmatrix} \tag{1}$$

where I denotes the identity matrix, 0 denotes the zero matrix, and Q is defined as

$$Q = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ & & \vdots & \\ 1 & 0 & \cdots & 0 \end{bmatrix}.$$

Application 2 For each vector $\delta = (i_1, \ldots, i_s) \in V_s$, we define a function D_δ on V_s in the following way:

$$D_\delta(y) = (y_1 \oplus \bar{i_1}) \ldots (y_s \oplus \bar{i_s})$$

where $y = (y_1, \ldots, y_s)$ and $\bar{i}$ denotes the binary complement of i, namely, $\bar{i} = 1 \oplus i$.

Using this notation, we define the "concatenation" of 2^s functions on V_t as follows:

$$f(y, x) = \bigoplus_{\delta \in V_s} D_\delta(y) g_\delta(x) \oplus r(y) \tag{2}$$

where $x = (x_1, \ldots, x_t)$, each g_δ is a function on V_t, and r is an arbitrary function on V_s. Of particular interest is the concatenation of linear functions on V_t. In Theorems 4 and 5 of [9], the following result is proved:

Lemma 1 *When $t \geqq s$ and all g_δ, $\delta \in V_s$, are distinct nonzero linear functions on V_t, the function f constructed by (2) is highly nonlinear and balanced. In addition, $f(z) \oplus f(z \oplus \gamma)$ is balanced for all $\gamma = (\beta, \alpha)$ with $\beta \neq 0$, where $z = (y, x)$, $\beta \in V_s$ and $\alpha \in V_t$.*

Let A be a nondegenerate matrix of order $s + t$. Suppose that the ith row γ_i of A can be written as $\gamma_i = (\beta_i, \alpha_i)$ with $\beta_i \neq 0$, where $\beta_i \in V_s$ and $\alpha_i \in V_t$. Then by Theorem 1, $\psi(z) = f(zA)$ satisfies the SAC. Note that the matrix A defined by (1) satisfies the requirements.

3 A Set of Functions

In computer security practice, such as the design of S-boxes, we often consider a set of functions. It is desirable that all component functions in a set simultaneously satisfy the SAC. ¿From Theorem 1 we can see that given a set of functions on V_n, $\{f_1, \ldots, f_m\}$, if A is a nondegenerate matrix of order n such that $f_i(x) \oplus f_i(x \oplus \gamma_j)$ is balanced for every function f_i and every row γ_j in A, then $g_1(x) = f_1(xA)$, ..., $g_m(x) = f_m(xA)$ all satisfy the SAC. The following theorem gives a sufficient condition for the existence of such a nondegenerate matrix.

Theorem 2 *Let f_1, ..., f_m be functions on V_n. Denote by B the set of vectors γ in V_n such that $f_j(x) \oplus f_j(x \oplus \gamma)$ is* not *balanced for some $1 \leqq j \leqq m$, and by $\#B$ the number of vectors in B. If $\#B < 2^{n-1}$, then there exists a nondegenerate matrix A of order n with entries from $GF(2)$ such that each $\psi_j(x) = f_j(xA)$ satisfies the SAC.*

Proof. We show how to construct a nondegenerate matrix A of order n, under the condition that $\#B < 2^{n-1}$. Denote by $S_{\alpha_1,\ldots,\alpha_k}$ the set of vectors consisting of all the linear combinations of vectors $\alpha_1, \ldots, \alpha_k$.

The first row of A, γ_1, is selected from V_n excluding those in B and the zero vector, i.e., from the vector set $V_n - B - S_0$. There are $2^n - \#B - 2^0$ different choices for γ_1. The second row of A, γ_2, is selected from the vector set $V_n - B - S_{\gamma_1}$. This guarantees that γ_2 is linearly independent of γ_1. We have $2^n - \#B - 2^1$ different choices for γ_2.

In general, once the first $k-1$ linearly independent rows γ_1, ..., γ_{k-1} of A are selected, the kth row γ_k, $k \leqq n$, will be selected from the vector set $V_n - B - S_{\gamma_1,\ldots,\gamma_{k-1}}$. This process ensures that γ_1, ..., γ_k are all linearly independent.

The number of choices for the last row γ_n is $2^n - \#B - 2^{n-1} = 2^{n-1} - \#B > 0$. Therefore, we can always find a nondegenerate matrix A such that $f_i(x) \oplus f_i(x \oplus \gamma_j)$ is balanced for every $1 \leqq i \leqq m$ and $1 \leqq j \leqq n$. By Theorem 1, $\psi_1(x) = f_1(xA)$, ..., $\psi_m(x) = f_m(xA)$ all satisfy the SAC. □

Theorem 2 has been applied in [10] to design S-boxes that possess many desirable cryptographic properties, which include the high nonlinearity, the SAC, the balanced-

ness and the robustness against differential cryptanalysis. As is shown below, the transformation technique can also be applied to other approaches to the construction of S-boxes.

Application 3 With the S-boxes studied in [6, 5, 3] each component function f_j has the following property: $f_j(x) \oplus f_j(x \oplus \alpha)$ is balanced for all but one nonzero vector $\alpha \in V_n$, where $x = (x_1, \ldots, x_n)$ and $n \geqq 3$ is odd. Thus we have $\#B \leqq n$. By Theorem 2 we can use a nondegenerate matrix to transform all the component functions of such an S-box into SAC-fulfilling ones.

4 A Final Remark

In [13], we have constructed highly nonlinear balanced functions on V_{2k+1} that satisfy the propagation criterion of degree $2k$ [8], and highly nonlinear balanced functions on V_{2k} that satisfy the propagation criterion of degree $\frac{4}{3}k$. A transformation technique similar to that presented in this paper has played an important role in the constructions.

References

[1] C. M. Adams and S. E. Tavares. The use of bent sequences to achieve higher-order strict avalanche criterion. Technical Report, TR 90-013, Department of Electrical Engineering, Queen's University, 1990.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.

[3] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[4] R. Forré. The strict avalanche criterion: Special properties of boolean functions and extended definition. In *Advances in Cryptology - CRYPTO'88*, volume

403, Lecture Notes in Computer Science, pages 450–468. Springer-Verlag, Berlin, Heidelberg, New York, 1989.

[5] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, volume Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 1992. to appear.

[6] J. Pieprzyk. Bent permutations. In *Proceeding of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing*, Las Vegas, 1991.

[7] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[8] B. Preneel, W. V. Leekwick, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[9] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[10] J. Seberry, X. M. Zhang, and Y. Zheng. Systematic generation of cryptographically robust S-boxes. In *Proceedings of the First ACM Conference on Computer and Communications Security*, November 1993. to appear.

[11] A. F. Webster. *Plaintext/Ciphertext Bit Dependencies in Cryptographic System*. Master's Thesis, Department of Electrical Engineering, Queen's University, 1985.

[12] A. F. Webster and S. E. Tavares. On the designs of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.

[13] X. M. Zhang, J. Seberry, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. Technical Report, Preprint No. 93-5, Department of Computer Science, University of Wollongong, 1993.